REMARKS

In the Official Action mailed on **20 December 2007**, the Examiner reviewed claims 1-25. Examiner rejected claims 1, 2, 7, 8, 13, 16, and 17 under 35 U.S.C. § 103(a) based on Hermann, Reto (EPO Publication No. EP1024626A1 hereinafter "Hermann") and Mizikovsky (U.S. Pat. No. 5,748,734 hereinafter "Mizikovsky"). Examiner rejected claims 3-6, 12, 14, 18-20, and 25 under 35 U.S.C. § 103(a) based on Hermann, Mizikovsky, and Harrisville-Wolff et al. (U.S. Pub. No. 2004/0030887 hereinafter "Harrisville-Wolff"). Examiner rejected claims 10, 11, 23, and 24 under 35 U.S.C. § 103(a) based on Hermann, Mizikovsky, Thompson et al. (U.S. Pub. No. 2002/0022483 hereinafter "Thompson"), and Harrisville-Wolff.

Rejections under 35 U.S.C. § 103(a))

Claims 1, 2, 7, 8, 13, 16, and 17 were rejected under Hermann and Mizikovsky. Applicant respectfully disagrees. Applicant points out that Mizikovsky discloses creating a cryptographic key for communication between a base station and a selected wireless terminal by communicating a first seed using a first communications channel, and communicating a second seed using a second communications channel (see Mizikovsky, col. 7, lines 43-44 and 49-50, and col. 8, lines 59-62). Thus, the two channels are **both used** for the purpose of establishing a secure communication between the two network nodes.

In contrast, embodiments of the present invention use the first communication channel **exclusively to establish secure communication** between the provisioning device and the network device, where this secure communication may then be conducted using a second non-preferred channel (see paragraph [0090] of the specification). In these embodiments, only the preferred channel is required to demonstrate identification and authenticity properties such as proximity between the provisioning device and the network device (see paragraphs [0052] – [0054] of the instant application). The second channel need not be location-limited.

This also finds support in paragraphs [0109]– [0112] of the specification in an application of an embodiment of the invention, using wireless sensors to monitor medical patients. In this embodiment, the wireless sensors on a patient are first configured at an enrollment station within the hospital (i.e., the location-limited preferred channel), where the configuration information include security information as well as other configuration information. This is followed by communicating patient data from the wireless sensors on the patient in a secure manner (i.e., using the non-location limited second channel), and now the patient with the wireless sensors need not be near the enrollment station.

This is beneficial because in these embodiments, the preferred channel can be used to send just enough provisioning information to bootstrap **subsequent secure communication** between the network device and the provisioning device. This allows for flexibility in terms of mobility for the network device because, when the network device has completed bootstrapping, the channel of communication between the network device and the provisioning device can be the second channel. The second channel does not require a close physical context such as is required by the preferred channel to enable communication (e.g., infrared signals, short wires, or audio signals), so using the second channel can significantly increase mobility, while ensuring secure communication.

There is nothing, either explicit or implicit, in the combined system of Hermann and Mizikovsky that describes the use of a preferred channel that has a proximity property **and that is exclusively used to exchange provisioning information, and thereby secure a non-preferred second channel for**

exchanging other information. The system of Hermann requires that **communication between the devices use a channel that is proximity-based** (see paragraph 35, lines 52-53 of Hermann). The system of Mizikovsky uses both channels to secure the communication between the devices, and thus, in combination with the system of Hermann, will require both channels to be proximal. It is not possible to use the system of Herman and Mizikovsky to bootstrap secure communication between the network device and the first device using only a first proximity based channel **and also securely exchange further information that uses a second channel that need not be proximal.**

Accordingly, Applicant has amended independent claims 1, 13, and 16 to clarify that a preferred channel that is a location-limited channel with a demonstrative identification property and an authenticity property; and where a first set of provisioning information is used to establish this secure and authenticated communication between the provisioning device and the network device using a second non-preferred channel. Dependent claims 7-8 and 21-22 have been canceled without prejudice. These amendments find support in paragraphs [0052]-[0054], [0090], and [0109]-[112] of the instant application. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 13, and 16 as presently amended are in condition for allowance. Applicant also submits that claims 2-6 and 9-12 which depend upon claim 1, claims 14-15, which depend upon claim 13, and claims 17-20 and 23-25, which depend upon claim 16, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By _/Shun Yao/________
Shun Yao
Registration No. 59,242

Date: 24 March 2008

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com